TEAMCENTER

Semiconductor Lifecycle Management — Deployment

Teamcenter 2412

SIEMENS

About Siemens Digital Industries Software

Siemens Digital Industries Software is a global leader in the growing field of product lifecycle management (PLM), manufacturing operations management (MOM), and electronic design automation (EDA) software, hardware, and services. Siemens works with more than 100,000 customers, leading the digitalization of their planning and manufacturing processes. At Siemens Digital Industries Software, we blur the boundaries between industry domains by integrating the virtual and physical, hardware and software, design and manufacturing worlds. With the rapid pace of innovation, digitalization is no longer tomorrow’s idea. We take what the future promises tomorrow and make it real for our customers today. Where today meets tomorrow. Our culture encourages creativity, welcomes fresh thinking and focuses on growth, so our people, our business, and our customers can achieve their full potential.

Support Center: **support.sw.siemens.com**

Send Feedback on Documentation: **support.sw.siemens.com/doc_feedback_form**

Contents

1. What is Teamcenter Semiconductor Lifecycle Management?

As the challenges facing the semiconductor industry increase in complexity, so does the design of the semiconductor devices that address them. Using Teamcenter Semiconductor Lifecycle Management software, you can track the complete product lifecycle and manage all metadata in a unified environment. Using a preconfigured semiconductor design and manufacturing BOM, you can streamline processes, workflows, and collaboration between designers and manufacturers to ensure data quality and compliance.

The solution focuses on the following three key aspects of the silicon lifecycle from design to manufacturing:

- New Product Introduction (NPI) manages the product delivery and spans the entire process from requirements capture to final product delivery.
- IC Design focuses on managing the Integrated Circuit (IC) design process and artifacts.
- IC Manufacturing focuses on the IC front-end and back-end manufacturing planning to enable foundry and back-end operations.

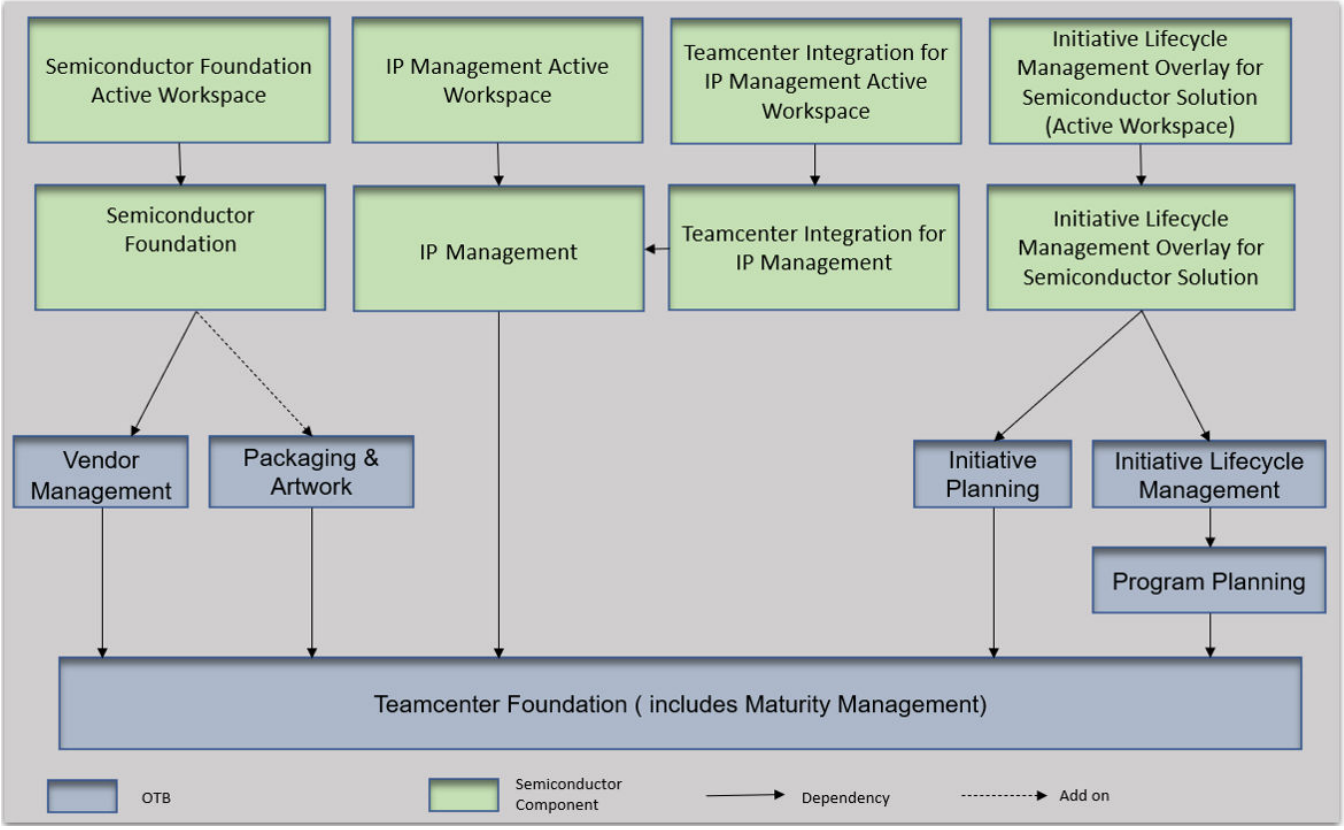
Where do I go from here?

 Business User	To manage the semiconductor design and manufacturing process and data, see Semiconductor Lifecycle Management — Usage.
 Administrator	
How do I install the Semiconductor Lifecycle Management solution using Deployment Center?	Refer to these **installation** steps to update your Teamcenter environment with the Semiconductor Lifecycle Management solution using Deployment Center.
What are some preferences that I can update to control behavior specific to the Semiconductor Lifecycle Management solution?	After installation is complete, there are several **preferences** to consider when configuring the Semiconductor Lifecycle Management solution.

2. Installation overview

Semiconductor Lifecycle Management can be installed into an existing environment that is running a supported version of Teamcenter. The solution is installed using **Deployment Center**. All required templates, data, and additional features, such as Program Planning, are installed with the Semiconductor Lifecycle Management solution.

3. Components and layers



4. Install using Deployment Center

Install Semiconductor Lifecycle Management using Deployment Center

Add Semiconductor Lifecycle Management to your existing Teamcenter environment through a series of tasks from selecting applications and entering configuration parameters to generating and running deployment scripts.

1. Log on to Deployment Center and select the environment to which you want to add Semiconductor Lifecycle Management.

2. Go to the **Applications** tab. Click **Add or Remove Selected Applications** .

3. In the **Available Applications** panel, use the web browser search to find and select the appropriate applications for installing the desired Semiconductor Lifecycle Management solution bundles based on the following table:

Solution Bundle	Applications
Semiconductor Foundation	Semiconductor Foundation
New Product Introduction	Initiative Lifecycle Management Overlay for Semiconductor Solution
Functional Safety	Functional Safety Analysis for Semiconductor Devices
IC Design	IP Management
IC Manufacturing	Consumer Packaged Goods > Consumer Products and Retail Foundation Consumer Packaged Goods > Packaging and Artwork Note: These two applications are automatically selected when the Semiconductor Foundation application is selected.
Methodics Integration	Teamcenter Integration for IP Management Note: **Install Active Integration Gateway** to use T4EA for integration with Methodics.
Reliability Testing	MBSE A La Carte > Parameter Management MBSE A La Carte > Requirements Management

Solution Bundle	Applications
	MBSE A La Carte > Test and Verification Management

Deployment Center automatically selects any additional dependent applications.

4. Select additional prerequisite applications from the following table based on the Semiconductor applications you are installing.

Semiconductor Lifecycle Management solution prerequisites	
	Audit Markup Note: Markup is automatically selected when the Requirements Management application is selected. Product Configurator Product Configurator Support for Active Content Structure Requirements Management
Easy Plan	Process Planning for BTO/BTS/CTO
Enterprise Knowledge Foundation	Dispatcher Client for Rich Client
Extensions	Dispatcher Product Configurator Product Configurator Support for Structure Manager
Manufacturing Process Management	Work Instructions
Reuse and Standardization	Library Management

5. Click **Update Selected Applications**.

6. Go to the **Components** tab, and in the **Selected Components** list, note any components whose configuration status is not **100%**. Select each incomplete component, enter required parameters, and save component settings until all components in the environment show a configuration status of **100%**.

   When all components are fully configured, the **Deploy** tab is enabled.

7. When you finish entering values for the incomplete components, click **Save Component Settings**.

8. Go to the **Deploy** tab. Click **Generate Install Scripts** to generate deployment scripts you will use to update affected machines.

   When script generation is complete, note any special instructions in the **Deploy Instructions** panel.

9. Locate deployment scripts, copy each script to its target machine, and then run each script on its target machine.

   For more information about running deployment scripts, see *Deployment Center — Usage*.

Install Active Integration Gateway

> Note:
>
> Before you begin, check version **compatibility** between Teamcenter and Active Integration Gateway (T4EA).

To deploy T4EA using Deployment Center:

1. Download and extract Active Integration Gateway and Teamcenter Gateway for Enterprise Application kits to your Deployment Center repository location. Select the version in accordance with your Teamcenter platform version.

2. Start Deployment Center and ensure the Active Integration Gateway and Teamcenter Gateway for Enterprise Applications products are visible under the **SOFTWARE REPOSITORIES** tile.

3. From the **Environments** tile, navigate to the location of your environment.

4. Go to the **Software** tab. Select **Active Integration**, **Active Integration for Active Workspace**, **Active Integration Gateway Foundation Services**, **Active Integration Gateway ITK for TC <version>**, **Integration Gateway T4EA**, and **Teamcenter Gateway for Enterprise Applications** from the **Available Software** panel, and then click **Update Selected Software**.

5. Go to the **Applications** tab. Click **Add or Remove Selected Applications**.

6. In the **Available Applications** panel, use the web browser search to find and select the following applications:

   - **Gateway Service – Basis**
   - **ITK**
   - **T4EA Gateway Service**
   - **Teamcenter Gateway for Enterprise Applications**

Deployment Center automatically selects any additional dependent applications.

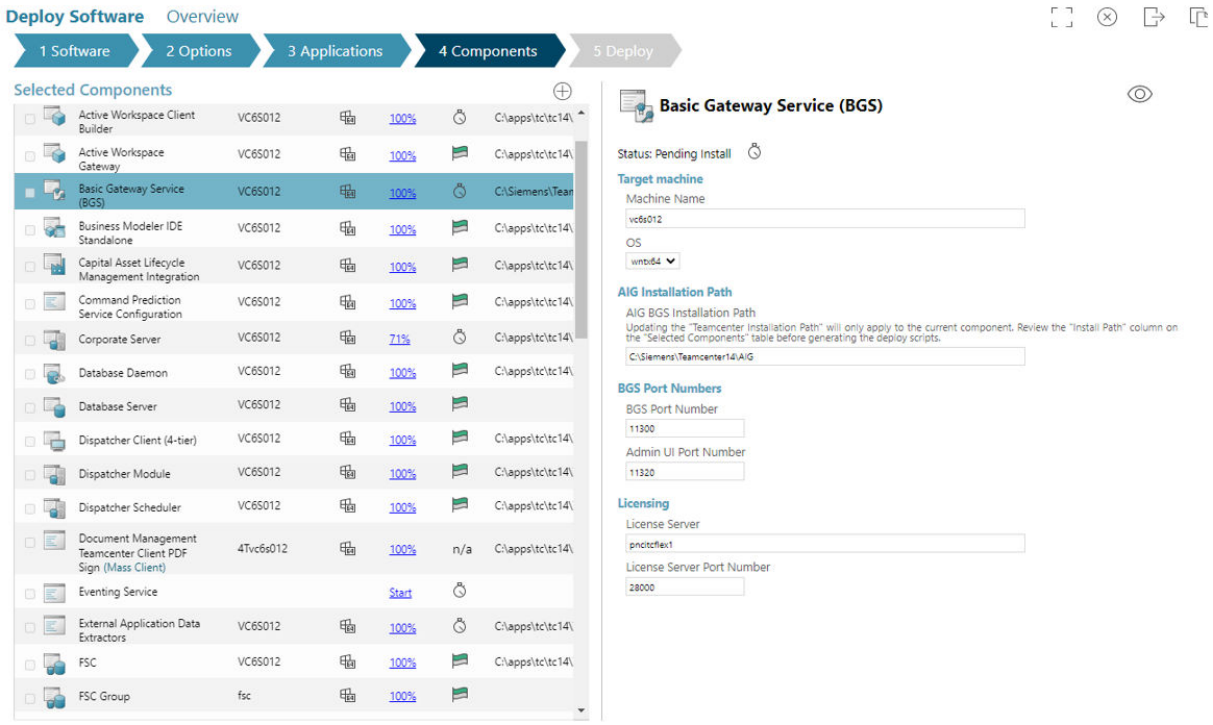
7. Click **Update Selected Applications**.

8. Go to the **Components** tab.

9. Configure the AIG components:

   a. In the **Selected Components** list, select Basic Gateway Service (BGS).

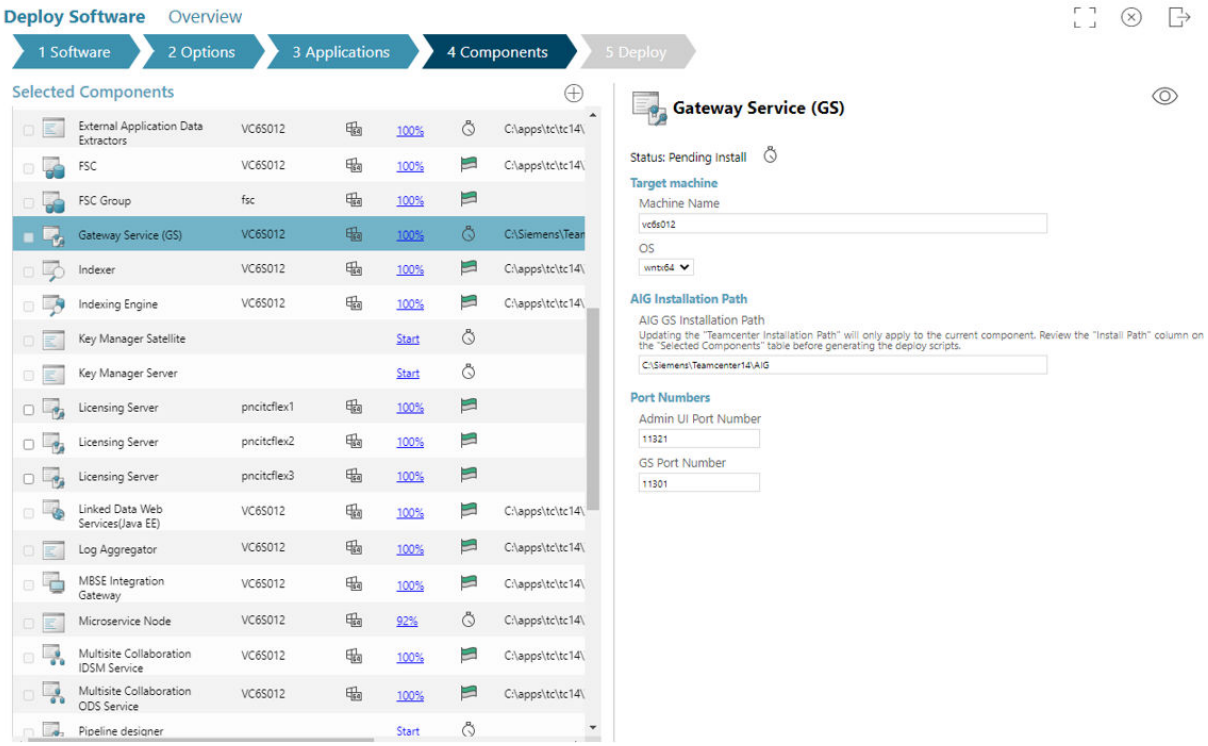
   b. In the Basic Gateway Service (BGS) panel, enter values for the configuration parameters.



   c. When you finish entering values for the Basic Gateway Service (BGS) component, click **Save Component Settings**.

   d. In the **Selected Components** list, select Gateway Service (GS).

   e. In the Gateway Service (GS) panel, enter values for the configuration parameters.



f. When you finish entering values for the Gateway Service (GS) component, click **Save Component Settings**.

g. In the **Selected Components** list, note any remaining components whose configuration status is not **100%**. Select each incomplete component, enter required parameters, and save component settings until all components in the environment show a configuration status of **100%**.

When all components are fully configured, the **Deploy** tab is enabled.

10. Go to the **Deploy** tab. Click **Generate Install Scripts** to generate deployment scripts you will use to update affected machines.

When script generation is complete, note any special instructions in the **Deploy Instructions** panel.

11. Locate deployment scripts, copy each script to its target machine, and then run each script on its target machine.

For more information about running deployment scripts, see *Deployment Center — Usage*.

5. Post install steps

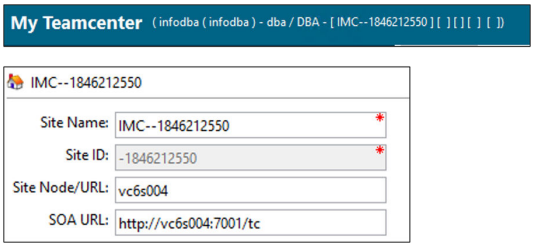
Organization changes

Update site information

Update the site URL to the web tier Teamcenter URL, for example, **http://servername:port_number/context_name**.

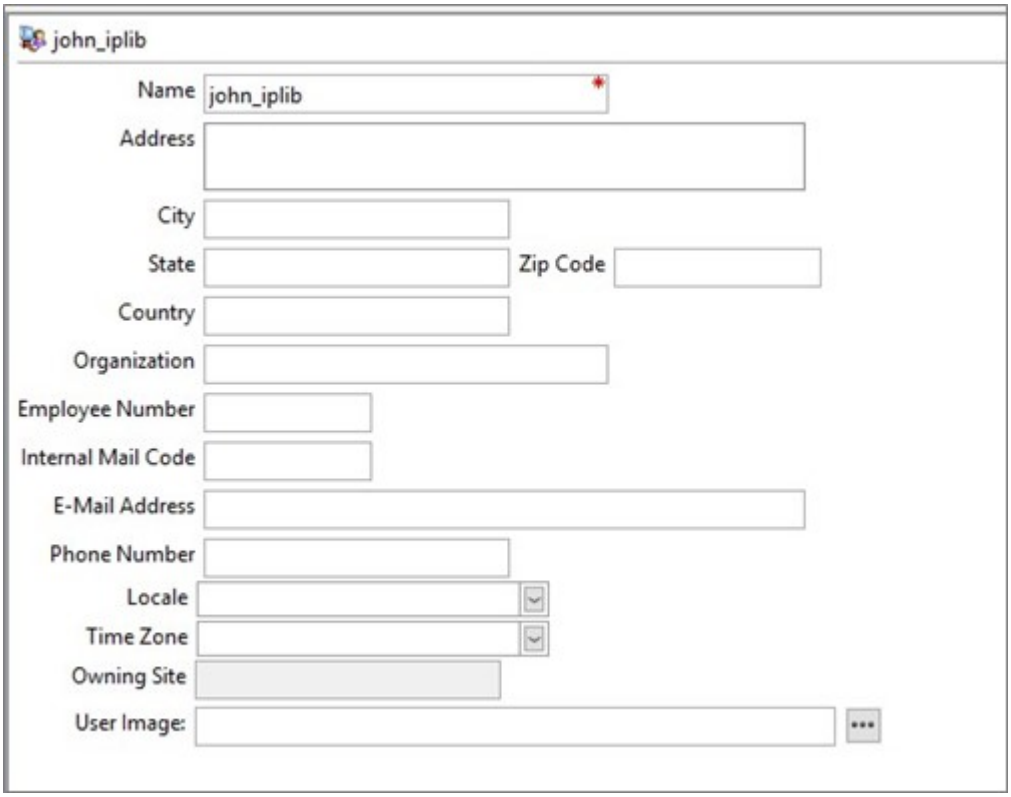
1. In the Teamcenter Organization application, select a site.

2. Type a site name in the **Site Name** box and the web tier URL in the **SOA URL** box.

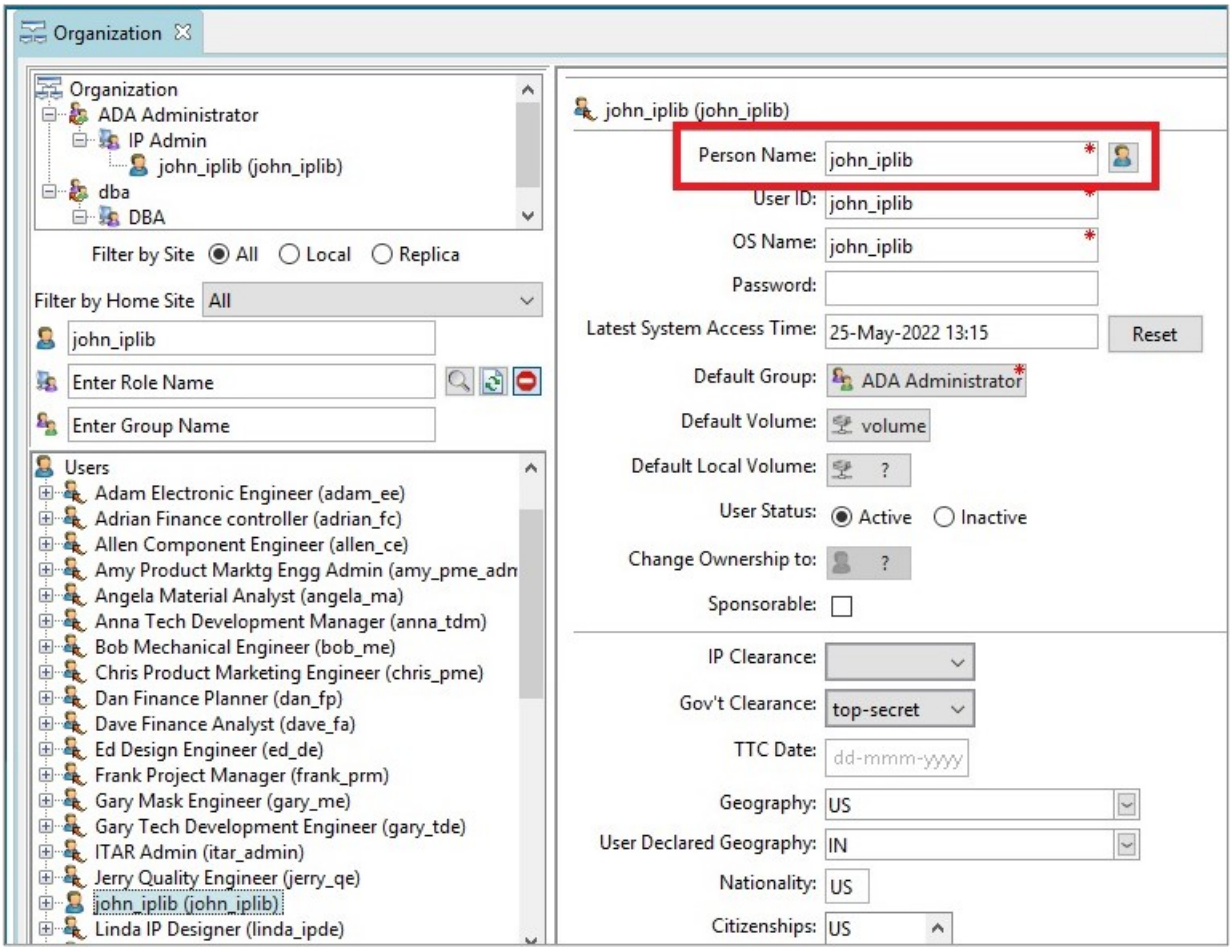


Update IP Librarian user

1. In the **Organization** application, create a new IP Librarian user.



2. Search for and select the IP Librarian user, and then update the **Person Name**.

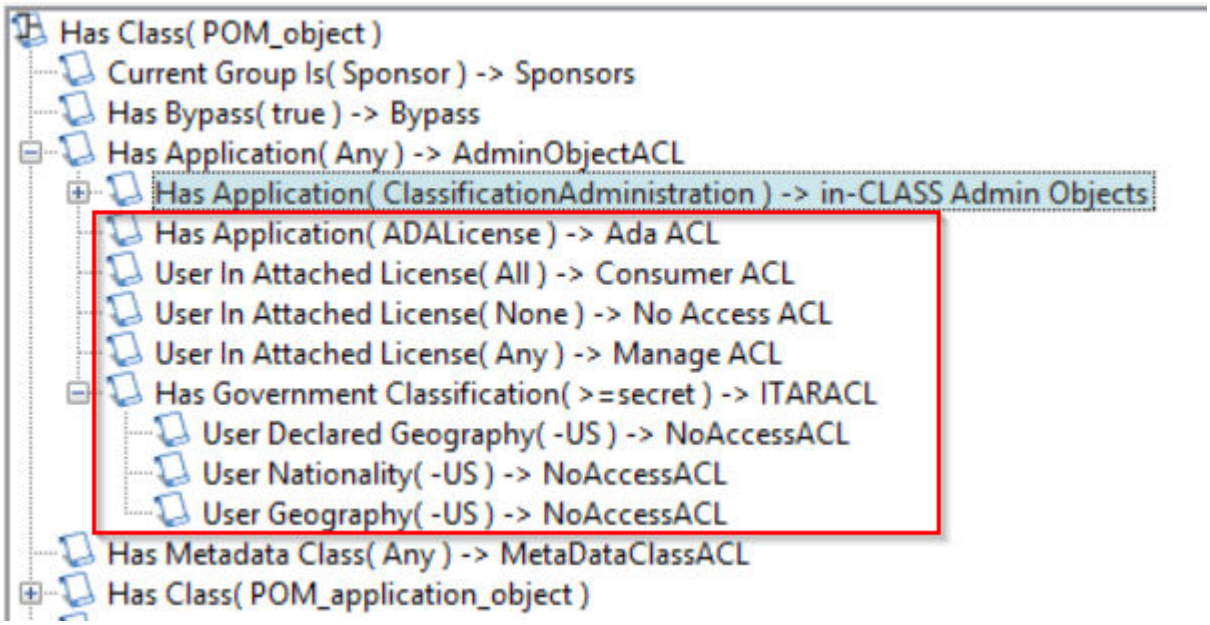


Update access control

1. Log into the Teamcenter rich client as an administrator and open the Access Manager application.

2. Create the ACLs shown below to support ITAR configurations. Be sure to add these ACLs immediately below the **Has Application (ClassificationAdministration) -> in-CLASS Admin object** in the ACL tree.

> Note:
>
> If accessor /roles are not available, then you must create them manually.



- ACL Name: **Ada ACL**

Type of Accessor	ID of Accessor	Grant	Deny
Group	ADA Administrator	Read Write Delete Change Copy Administer ADA Licenses Create	

- ACL Name: **Consumer ACL**

Type of Accessor	ID of Accessor	Grant	Deny
User Under Government Clearance			Read
User Has Government Clearance		Read	
User Over Government Clearance		Read	

Type of Accessor	ID of Accessor	Grant	Deny
Role in Owning Group	IP Admin	Unmanage IP Admin ITAR Admin	
Role in Owning Group	ITAR Admin	Unmanage IP Admin ITAR Admin	

- ACL Name: **No Access ACL**

Type of Accessor	ID of Accessor	Grant	Deny
Role in Owning Group	IP Admin	Unmanage IP Admin ITAR Admin	
Role in Owning Group	ITAR Admin	Unmanage IP Admin ITAR Admin	
World			Read

- ACL Name: **Manage ACL**

Type of Accessor	ID of Accessor	Grant	Deny
User Under Government Clearance			Read
User Has Government Clearance			Read
User Over Government Clearance			Read
Role in Owning Group	IP Admin	Unmanage IP Admin ITAR Admin	
Role in Owning Group	ITAR Admin	Unmanage IP Admin	

Type of Accessor	ID of Accessor	Grant	Deny
		ITAR Admin	
World			Read

- ACL Name: **ITARACL**

Type of Accessor	ID of Accessor	Grant	Deny
User Under Government Clearance			Read
User Has Government Clearance		Read	
User Over Government Clearance		Read	
Role in Owning Group	IP Admin	Unmanage IP Admin ITAR Admin	
Role in Owning Group	ITAR Admin	Unmanage IP Admin ITAR Admin	
World			Read

- ACL Name: **NoAccessACL**

Type of Accessor	ID of Accessor	Grant	Deny
World			Read

Preference changes

1. Set the classification preferences.

   Update the preference values to **true** for the following classification preferences:

   - **CLS_is_presentation_hierarchy_active**
   - **CLS_auto_sync_node_hierarchy**
   - **ICS_searchindex_view_visible**

2. Run the **clsutility** utility to update existing classes with presentation layer classification.

```
clsutility.exe -u=<user-id> -p=<password> -g=<group> -import
-hierarchy -cid=ICM -include_instances
```

3. Set the reliability testing preferences.

   Update the preference values to **true** for the following preferences:

   - **PLE_Parameter_Create_With_Definition_Ux**
   - **PLE_Parameter_Create_With_Application_Ux**

4. Set test kit BOM validation preferences.

5. Update the **SUBSCMPLAW_ComplianceCheck_Command_SupportedTypes** preference by appending the following value:

   Sfd0PackageKitRevision

   > Note:
   >
   > This preference only needs to be updated if Substance Compliance functionality is being used.

6. To allow sharing a safety goal across multiple HARA analyses for the same part, set the **Fs0Allow_SafetyGoal_On_MultipleHARA** preference value to **true**.

   > Note:
   >
   > Sharing a safety goal across multiple HARA analyses for different parts is always prohibited.

7. Set the advanced packaging preferences.

   - Update the **TCAllowedChildTypes_***<Object_Type>* preference to choose the object types listed in the create panel.
   - Update the **Sfd0_Auto_Classification_Class_Ids** preference to define the mapping of attribute value and the classification class IDs used for automatically classifying an object at creation.

   If changes are made to the allowable child types, you must also update the relevant verification rule.

Condition Name	Object Type
Sfd0BOMValidationConditionForInterposerAssembly	Sfd0IntposerAsm
Sfd0BOMValidationConditionForDieKit	Sfd0DieKit
Sfd0BOMValidationConditionForPackageKit	Sfd0PackageKit

Post install steps for Easy Plan

1. Remove the existing values and add the following values to the **EP_SearchSubtypesForMbom** preference:

   - **Sfd0SingulatdDieRevision**
   - **Sfd0AssemblyPartRevision**

2. Remove the existing values and add the following values to the **EP_ProcessPageTabProcessAreaColumnConfiguration** preference:

   - **ImanItemBOPLine.bl_sequence_no**
   - **ImanItemBOPLine.bl_quantity**

3. Remove the existing values and add the following values to the **EP_SearchSubtypesForEbom** preference:

   - **Sfd0DieDesignRevision**

4. Remove the existing values and add the following values to the **EP_WorkPackageContentType** preference:

   - **Product:Item**
   - **Plant:Item**
   - **PlantBOP:Item**

5. Set the **EP_PlanningForSmallProduct** preference to **True**.

6. Set the **EP_ShowOnlyEWI** preference to **False**.

7. Set the **EP_EnableLineBalancing** preference to **False**.

8. Install the **New Work Package** tile for Semiconductor workspaces.

a. Locate the *Sfd1semiconductorfoundationawTilesCots_Install.xml* file in the Teamcenter kit location, *tc\sfd1semiconductorfoundationaw_samples\samples*.

b. In a TC command prompt window, run the following command:

```
aws2_install_tilecollections -u=<user-id> -p=<password>
-g=<group> -mode=add -file=<DIRECTORY_OF_TC_KIT>/tc/
sfd1semiconductorfoundationaw_samples/samples/
Sfd1semiconductorfoundationawTilesCots_Install.xml
```

> Note:
>
> You must be an administrator to run this command.

Sample class hierarchy

> Note:
>
> This task is optional.

Create a sample class hierarchy using the sample classification data provided with the foundation kit. Follow the instructions available at the following locations:

- in the *README.txt* file located at *${TC_INSTALL_DIR}/sfd1semiconductorfoundationaw/samples*
- in the Teamcenter kit located at *tc\sfd1semiconductorfoundationaw_samples\samples*

Post install steps for T4EA

1. Update **HOST** with the full computer name in the *%GS_ROOT%\var\conf\tpds.overlay* and *%BGS_ROOT%\var\conf\tpds.overlay* files.

2. Open a Teamcenter command prompt, go to the *%BGS_HOME%\bin64* directory, and run the **initpassword.exe** command to set the administrator password.

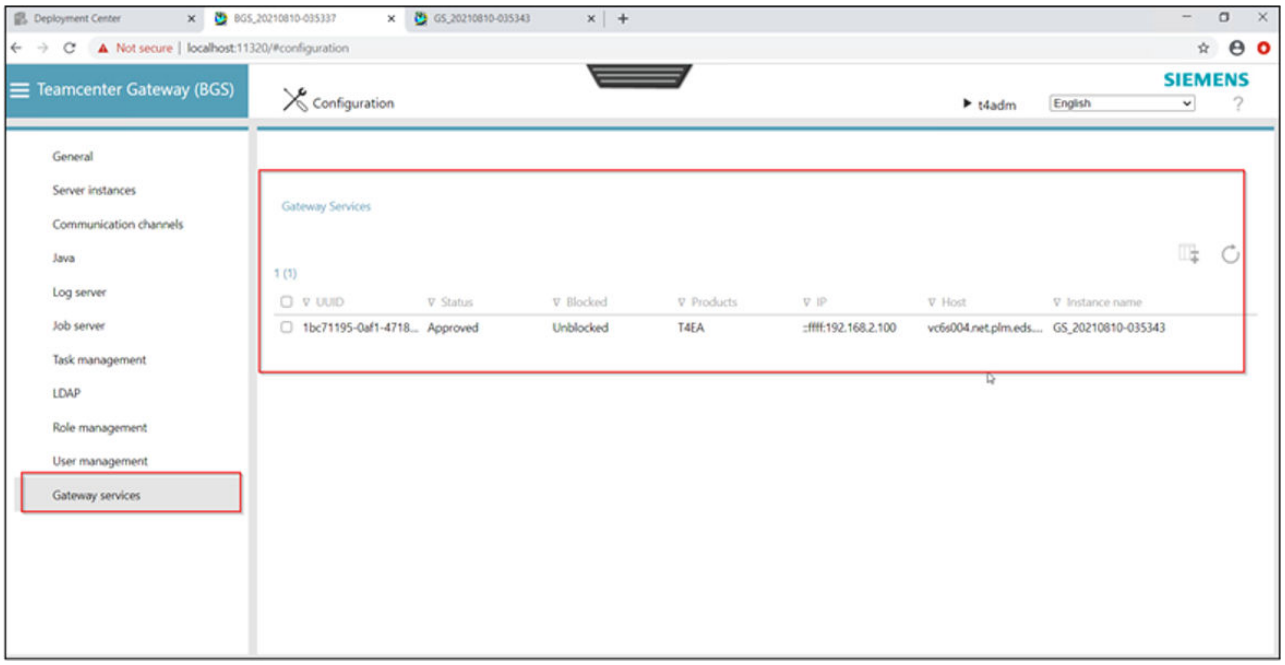
   In this example, the default admin user **t4adm** is used with a password of **t4adm**.

```
C:\apps\Siemens\ActiveIntegration\bgs\bin64>initpassword.exe
Copyright (c) 2019-2020 Siemens Product Lifecycle Management Software Inc. All rights reserved

       Password initializer for PL4x v0.0.8 6681

   Password must be passed via the environment variable T4ADM_SECRET or entered on the console

2021/08/10 06:55:10 Set up logging into 'C:\apps\Siemens\ActiveIntegration\bgs\tmp\initpassword.log' and the console.
Enter password (will not be shown): *****
Repeat password: *****
2021/08/10 06:55:25 UUID path: C:\apps\Siemens\ActiveIntegration\bgs\var\conf\uuid
2021/08/10 06:55:25 Created a new UUID
2021/08/10 06:55:25 Serving at address: 127.0.0.1:11399
2021/08/10 06:55:28 Starting to serve...
2021/08/10 06:55:28 Please start the BGS within 60 seconds now
2021/08/10 06:55:42 Password fetched by 'd9cbab53-bced-4825-a4a7-09e6749e9f9c' @ 127.0.0.1:64150. Exiting...

C:\apps\Siemens\ActiveIntegration\bgs\bin64>
```

3. Start services of Teamcenter Gateway (BGS) and Gateway Services (GS) from *%GS_ROOT%\bin64* and *%BGS_ROOT%\bin64* by running **start.exe**.

   - Go to the BGS login using **https://localhost:11320** and the GS login using **https://localhost:11321**. Log in with **t4adm** for the username and password.

4. Go to BGS, select the configuration, and click **Gateway services**. Confirm that the gateway service status is **Approved**.



Enable T4EA – Teamcenter integration flow

1. For a 2-tier client, edit the *%TC_ROOT%\iiopservers\start_TcServer1.bat* file and add an entry of **t4x_env.bat**.

```
Rem Begin
call %TC_DATA%\tc_profilevars
if not defined Transient_Volume_RootDir set Transient_Volume_RootDir=%USERPROFILE%\Local Settings\Temp\TransientDirs
if not exist "%Transient_Volume_RootDir%" mkdir "%Transient_Volume_RootDir%"
call E:\apps\Siemens\ActiveIntegration\gs\etc\t4x_env.bat

Rem Ok, now start it.
%TC_ROOT%\bin\tcserver.exe -ORBInitRef ImplRepoService=corbaloc:iiop:localhost:1572/ImplRepoService id=TcServer1 useImR -ORBUseIMR 1
goto :EOF

:TCROOT_error
echo *** ERROR ***
echo TC_ROOT does not exist or is NOT valid.
```

2. For a 4-tier client, edit the *%TC_ROOT%\pool_manager\confs\tcenv.bat* file and add an entry of **t4x_env.bat**.

```
    rem consumes the output. For debug purpose you may want to redirect the output to a file.
    call "%TC_DATA%\tc_profilevars.bat" > nul
) else (
    echo "%TC_DATA%\tc_profilevars.bat" not found when executing tcenv.bat >& 2
)

call E:\apps\Siemens\ActiveIntegration\gs\etc\t4x_env.bat

rem Indicate TC servers should exit for POM initialization errors
set TC_EXIT_FOR_POOL=1
```

Ensure that the *t4x_env.bat* file is located at *%GS_ROOT%\etc*.

> Note:
>
> These paths change based on the Active Integration (BGS and GS) Installation directory.

3. Edit the *%GS_ROOT%\var\conf\script\t4xcust.bat* and *%BGS_ROOT%\var\conf\script\t4xcust.bat* files and enable Teamcenter and T4EA variables as shown.

```
REM EXAMPLE tc_profilevars call
REM IF NOT "x%TC_DATA_MODEL%" == "x" goto p1
set TC_ROOT=C:\apps\Siemens\Teamcenter13\TR
set TC_DATA=C:\apps\Siemens\Teamcenter13\TD
call %TC_DATA%\tc_profilevars.bat
REM :p1
REM
```

> Note:
>
> These paths change based on the Teamcenter installation directory.

```
REM
set TP_T4XINSTL=E:\apps\Siemens\ActiveIntegration\gs

REM Please use bin32 if the Teamcenter server is using the 32 bi
REM otherwise use the bin64 in the PATH definition

REM set PATH=%TP_T4XINSTL%\bin32;%PATH%
REM or
set PATH=%TP_T4XINSTL%\bin64;%PATH%

REM SET USER TEMP DIRECTORY
set TP_UTMP=%TEMP%

REM optional - activated extended itk pipe debugging
REM not for production environments
set TP_PIPEDEBUG=1
```

Remove T4EA mapping files

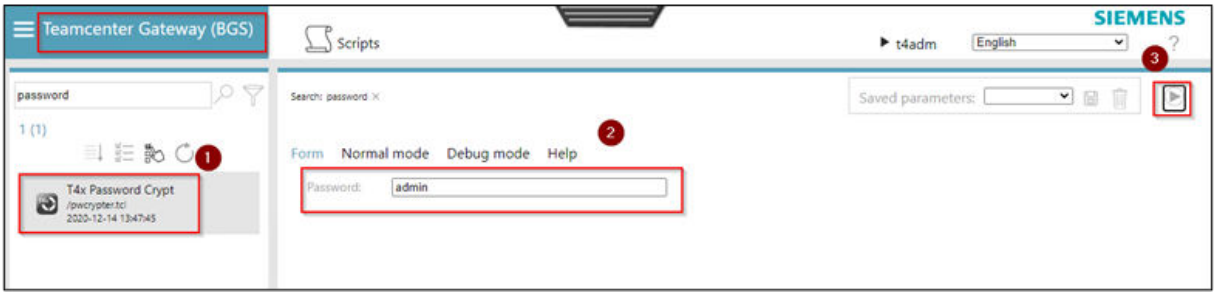
Navigate to the GS mapping files directory (*%GS_ROOT%\var\mmap*) and delete all out-of-the-box files.

1. Encrypt the password.

   a. In BGS, open the **T4x Password Crypt** script.

   b. Type **admin** in the **Password** box.

   c. Click **Run**.

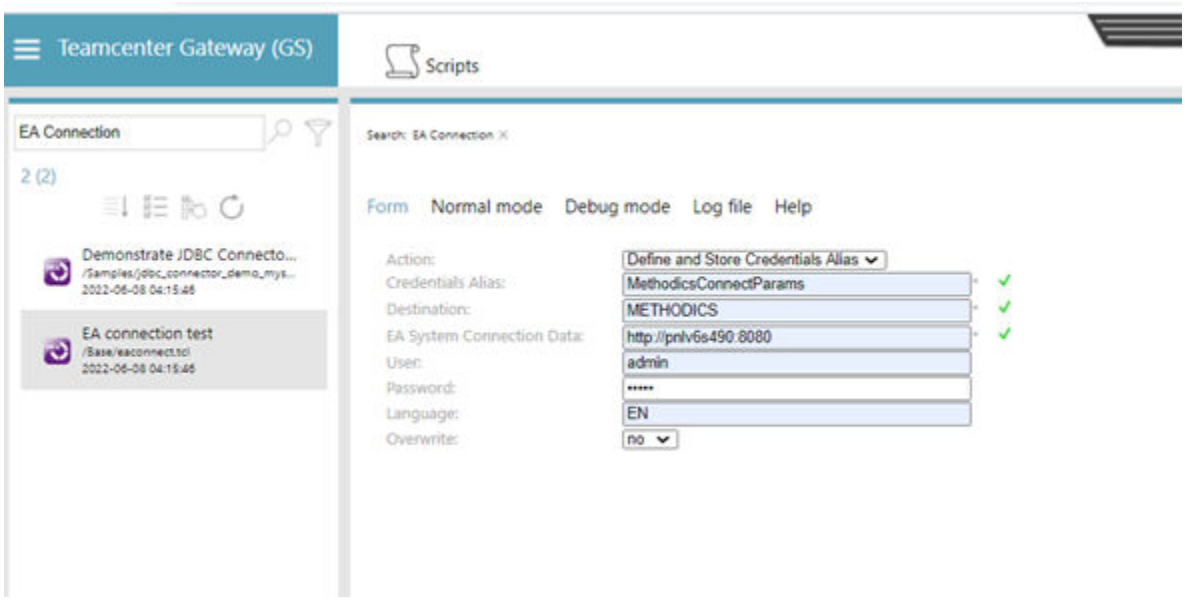


2. Update the mapping file.

Store connection information

In the GS administrator interface, run the EA connection test with the parameters as shown in the following graphic. For the **EA System Connection Data**, enter the URL where Methodics is available.

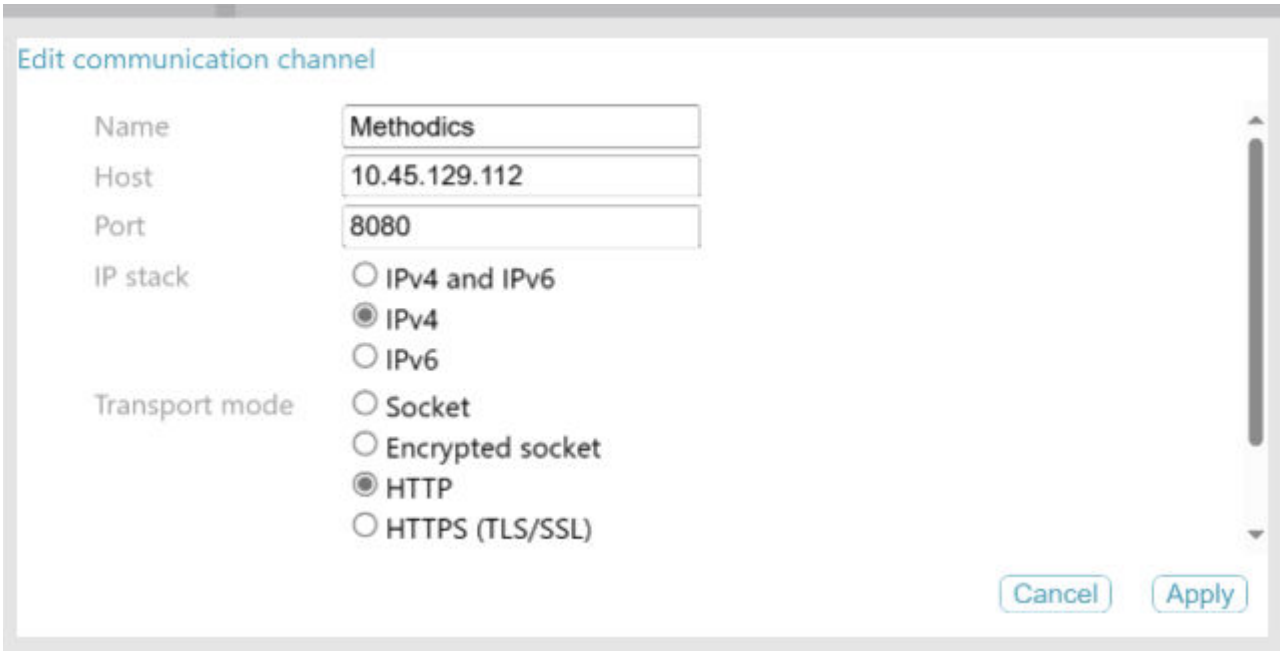
> Note:
>
> Type **METHODICS** in the destination box exactly as shown in the following image.



Add communication channels for Methodics in BGS and GS

1. In BGS, open the **Configuration** page.
2. Select the communication channel and click the plus (+).
3. Enter details according to the Methodics server information.

> Note:
>
> Type the channel **Name** exactly as shown in the following image.



4. In the same way, add a communication channel in the GS server.

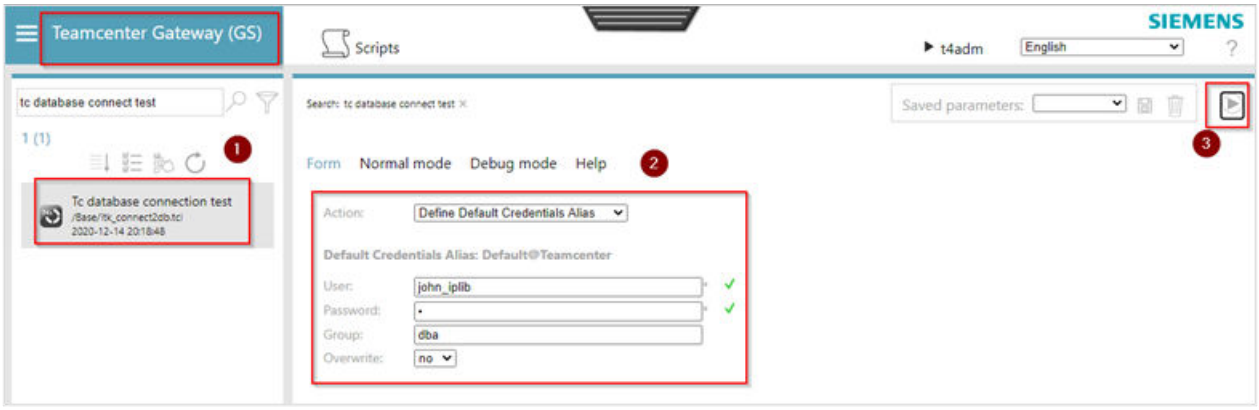
Create an alias

Register a Default and Librarian alias.

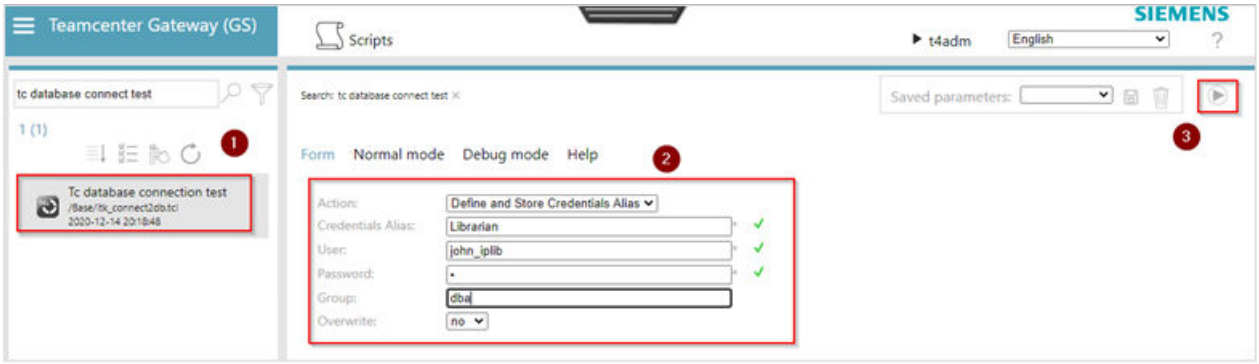
1. In GS, open the **Tc database connection test** script.

2. For the **Action**, select **Define Default Credentials Alias**.

3. Enter a username and password for the IP Administrator, and run the script.



4. Now enter a username and password for the Librarian, and run the script.



5. Open the *%TC_INSTALL_DIR%\ip0tc4ipmgmt\t4ea_configuration\GS\var\mmap\t4methodics_mapping_config\t4methodics_mapping_config.sd* file.

6. Make the following updates to the mapping file:

   - Specify the **TCServer HostName** in the **T4EA_Defaults(TCSERVERURL)** constant.
   - Specify the **TCServer PortNumber** in the **T4EA_Defaults(TCSERVERURL)** constant.

   Example:

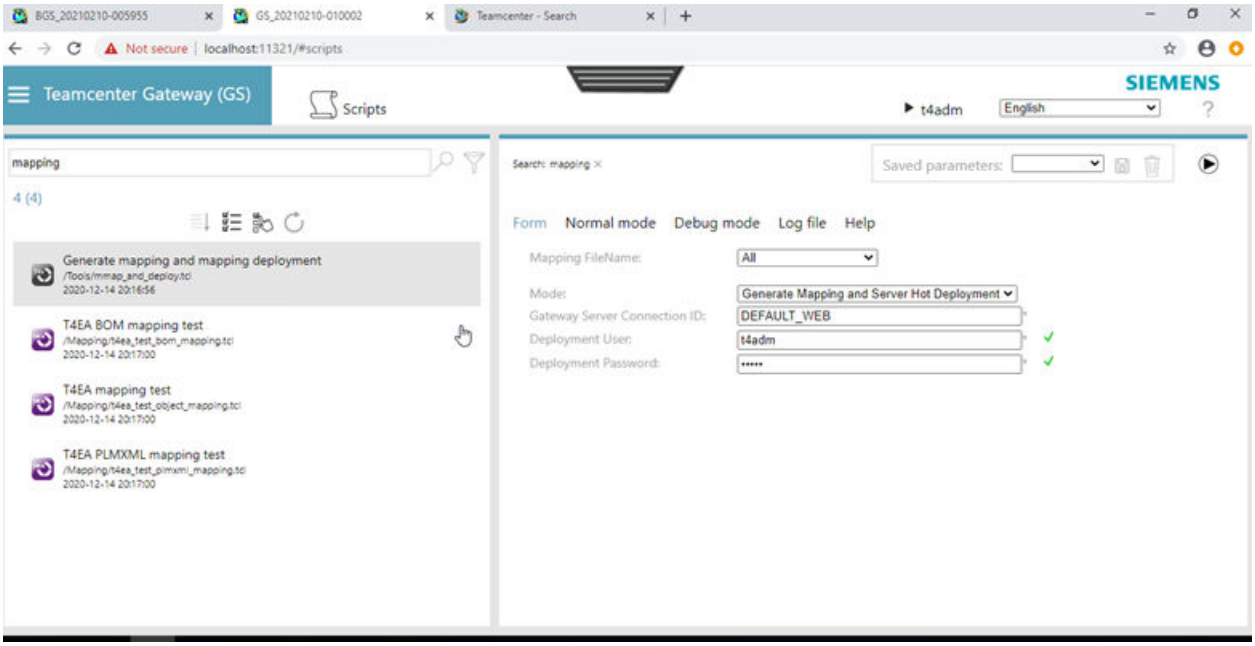
   ```
   set ::T4EA_Defaults(TCSERVERURL) http://10.134.54.4:3000
   ```

Deploy the mapping files

1. Copy *%TC_INSTALL_DIR%\ipt0tc4ipmgmt\businessdata\ipt0tc4ipmgmt\install\t4ea_configuration\GS\var\mmap\t4methodics_mapping_config* and *%TC_INSTALL_DIR%\ipt0tc4ipmgmt\businessdata\ipt0tc4ipmgmt\install\t4ea_configuration\GS\var\mmap\t4ea_mapping_config* to *%GS_ROOT%\var\mmap*.

2. In GS, select **Generate mapping and mapping deployment**.

3. Select **Generate Mapping and Server Hot Deployment** for the **Mode**, and enter the deployment username and password.



6. Administer Semiconductor Devices Lifecycle Management

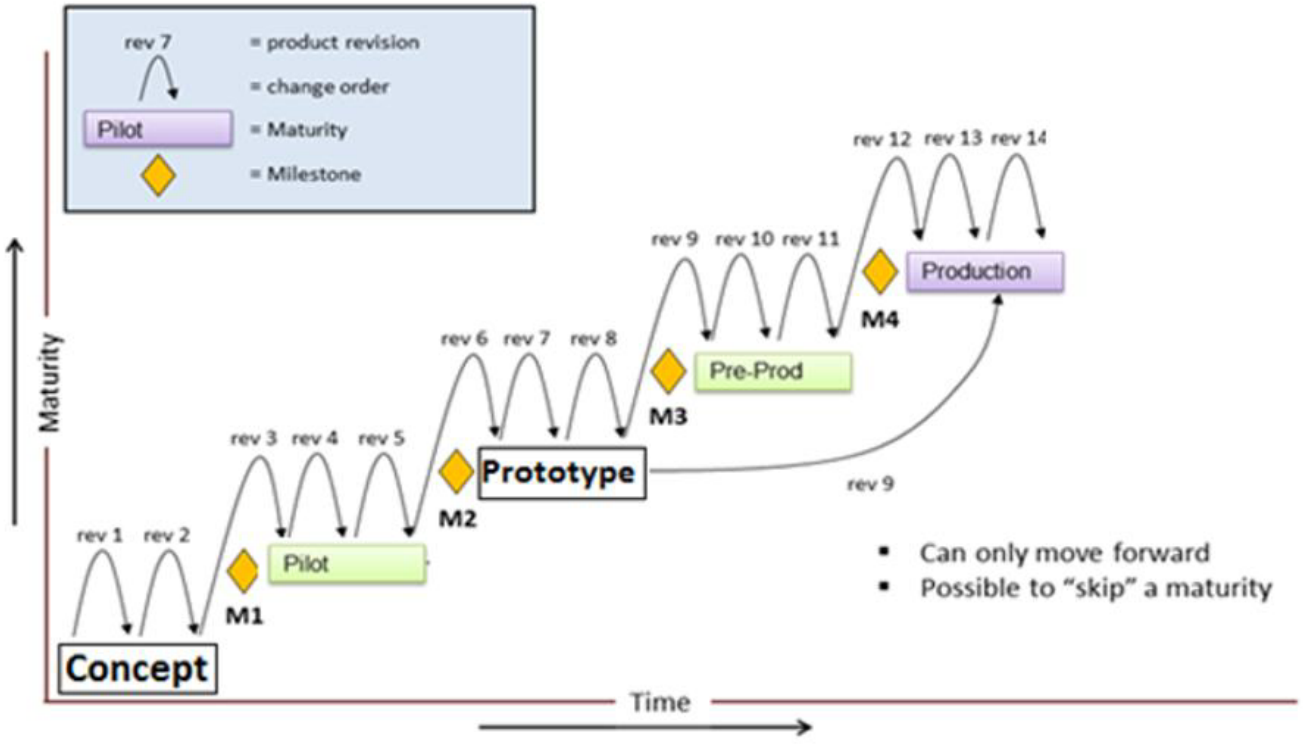
Maturity management

The Semiconductor Lifecycle Management solution enables you to control some capabilities by configuring them in Teamcenter.

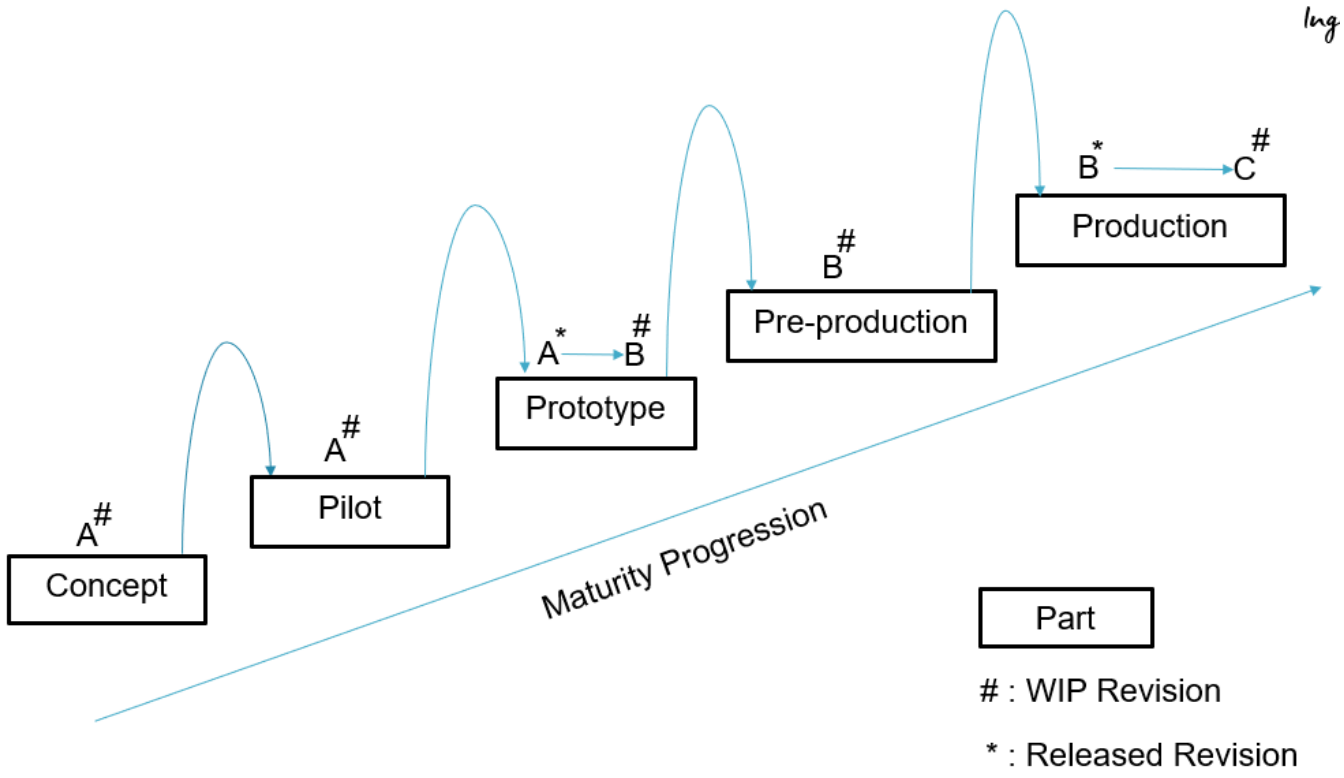
Maturity management

- Maturity describes the design maturity of a business object as it moves through its life.
- Maturity is a loose form of tracking the progression of a business object through its Maturity phases.
- Maturity and Release statuses may signify different levels of data sharing depending on the business rules of an organization.

For example, Maturity status **Pre-Production** may mean that the design organization can internally share data with its manufacturing organization, but the data cannot be shared externally with the suppliers unless it has been released with a Release Status of **Released**.



Example Maturity Progression for a Part



Progression rules

- For a specific business object, the evaluation of maturity progression should be configurable.
- Achieve configuration by the business object (**BO**) constant **Fnd0MaturityProgressionValidation**.

  Values for the BO constant are:

  1. No Maturity progression validation (default).
  2. Promote to any higher value and demotion is not allowed within the same working copy.
  3. Promote to any higher value and demotion up to based on previous revision's maturity value.
- The system performs the validation based on the **BO**'s business constant value.
- In the Semiconductor Lifecycle Management solution, all part revisions are configured with constant value **3**.
- Idea, IP Object Revision, and Semiconductor Qualification Revision are configured with constant value **1**.

Part Maturity rules

1. A new revision of a part carries over the Maturity value from the previous revision.

2. Skipping maturity levels is allowed.

BOM Maturity rules

1. The parent cannot be more mature than any of its immediate children. Validation is done by a workflow handler. The workflow handler can be used in any BOM Review and Release workflows.

2. In the Semiconductor Lifecycle Management solution, the **Validate-assembly-maturity-progression** rule handler is used in the start of the root task for the **Mask Set Release Process**.

Handler	Workflow template used in
Validate-assembly-maturity-progression Task:Start	**Mask Set Release Process**:Root

Validate-assembly-maturity-progression

A rule handler to check the Maturity state of a parent cannot be more mature than the Maturity state of its children.

Arguments:

rev_rule — Specifies the name of the revision rule to be applied for BOM traversal. If not supplied, the default revision rule is used.

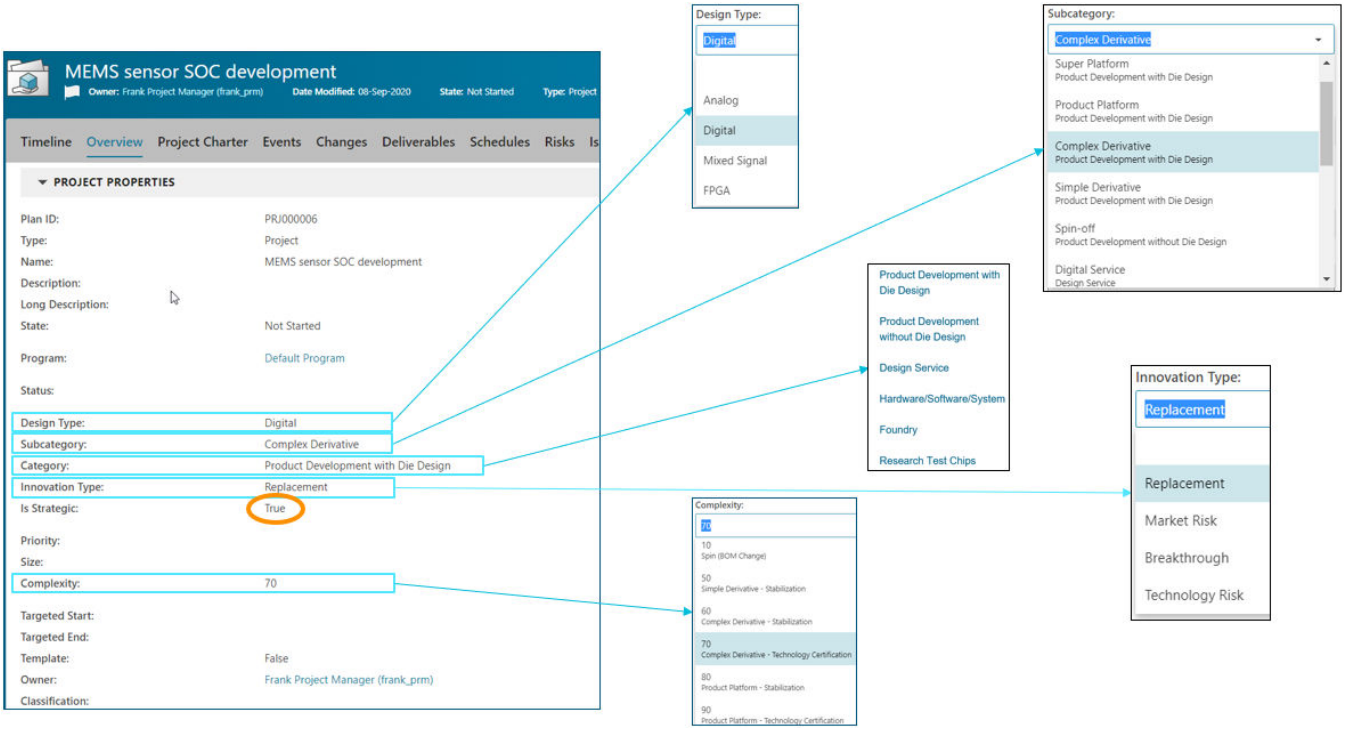
maturity_to_be_applied — Defines the Maturity state to be applied to the target object.

check_unconfigured — Returns **NO-GO** in case the applied revision rule on the assembly results in unconfigured children.

child_types_to_ignore — Defines the child types to be excluded from validation.

Project creation based on metadata

When a project is created, project parameters must be provided. The following image shows the method of configuring a project's properties using metadata.



There are many properties available on a project, such as **Design Type**, **Subcategory**, and **Innovation Type**. Another property that can be utilized is **Strategic**, which can be set to **True** or **False** and is used for prioritization and report filtering.

In many cases, prioritization is based on the expected revenue, the Net Present Value (NPV), or the Average Selling Price (ASP) of the product. However, there are some projects without a high NPV that are still a high priority. For example, foundation projects may be critical for use in other projects in the pipeline, so they must have high visibility and be executed on time.

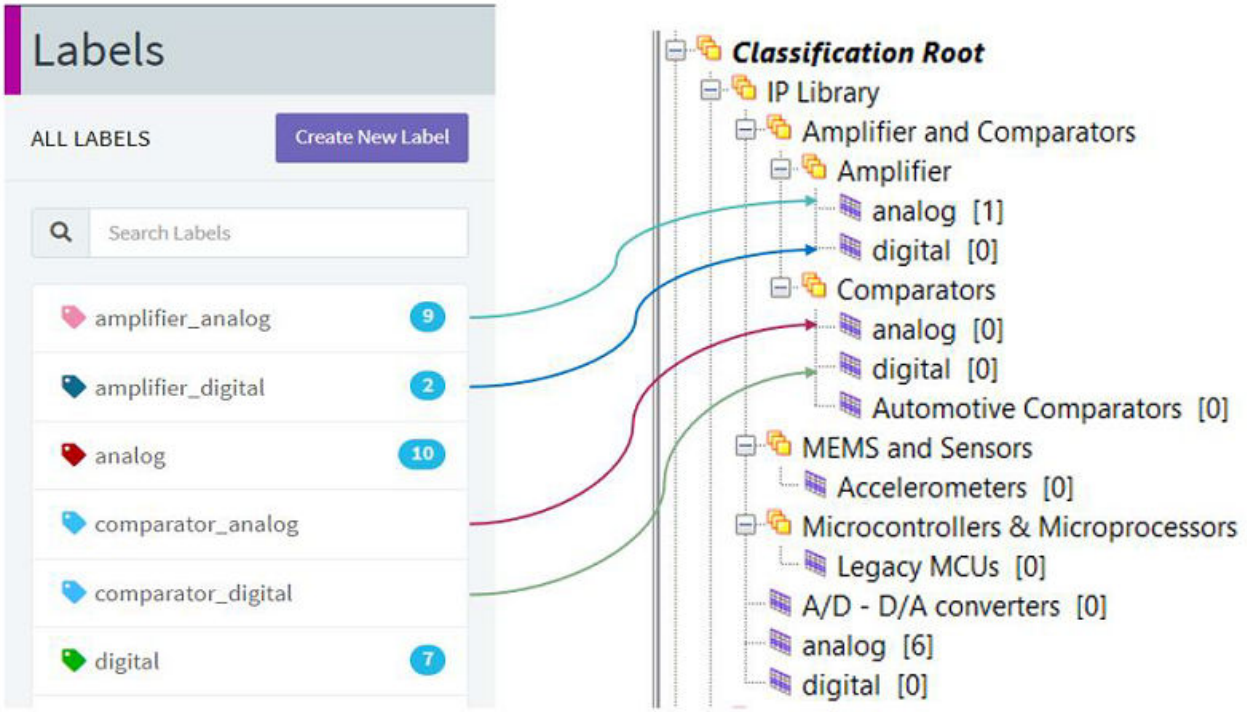
The **Strategic** property can be used for more flexible prioritization. A Top 10 Projects dashboard sorts by NPV by default, but projects with the **Strategic** property set to **True** may have equal priority. Dashboards can be configured to report based on your desired criteria.

These attributes drive the templates. You designate users to manage and enhance the templates based on your desired business process flows. Siemens Digital Industries Software has provided baseline templates and automated workflows to enable rapid deployment of the system.

Methodics configuration

This topic describes several data mappings from Methodics to Teamcenter.

- You can define the mapping of **Methodics** Labels and Teamcenter classification class IDs in the **IP_Classification_Class_id_mapping** preference.



- You can define the mapping of **Methodics** IP attributes and Teamcenter classification attribute IDs in the **IP_Classification_Attribute_id_mapping** preference.

- You can define the mapping of **Methodics** labels and **Methodics** properties set in the **IP_Label_Property_Set_mapping** preference. This preference is applicable only when exporting the **Bill of IP** defined for **Die Design** from Teamcenter.

- In the **Released_IP_Alias_Name** preference, you can define the released IP's alias name based on which IPVs should be imported to Teamcenter.

Test kit BOM validation configuration

Testing of semiconductors requires an electrical connection between the test head and the device handler. There are currently two methods used for coupling these two components:

1. “Hard” docking – Mechanical components physically lock the handler to the test head.

2. "Soft” docking – The test head and the handler are connected by a simple mating-type connector.

A connector is required in a test kit BOM only if there is a test interface board that contains “Soft” docking. There are validations to ensure this.

During addition or replacement of an item in a test kit, the validations ensure that a factory tool classified as a connector can only be added if the test kit BOM already contains an equipment item classified as a test interface board with the classification attribute **Docking Type** set to **Soft**.

The following preferences must be set to ensure the validations work correctly.

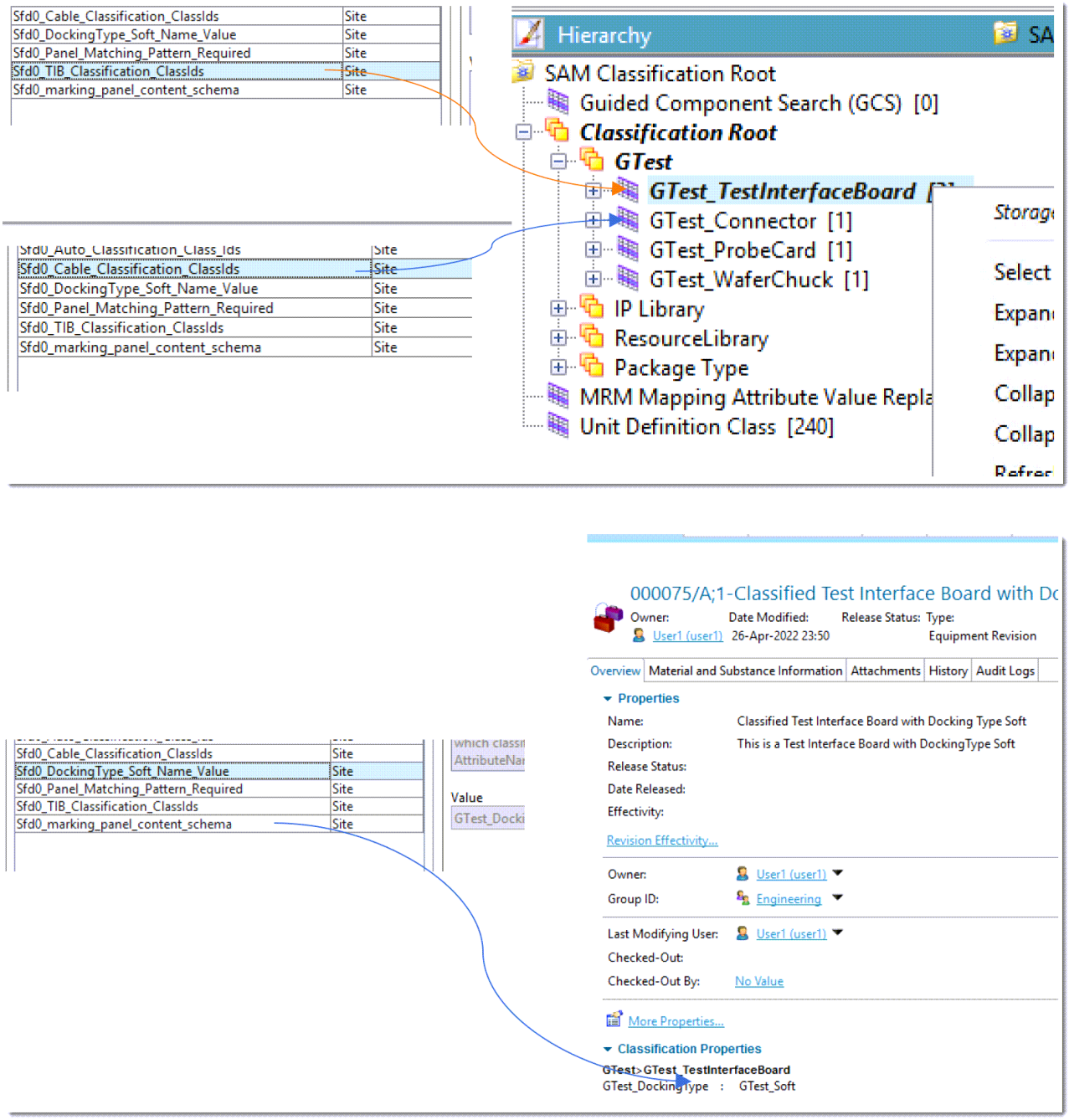
1. Set **Sfd0_Cable_Classification_ClassIds** to the classification class ID(s) of the **Cable/Connector** class.

2. Set **Sfd0_TIB_Classification_ClassIds** to the classification class ID(s) of the **Test Interface Board** class.

3. Set **Sfd0_DockingType_Soft_Name_Value** to the `name:attribute` value of the attribute that classifies a **Test Interface Board** as **Soft**.

   Example:

   DockingType:Soft



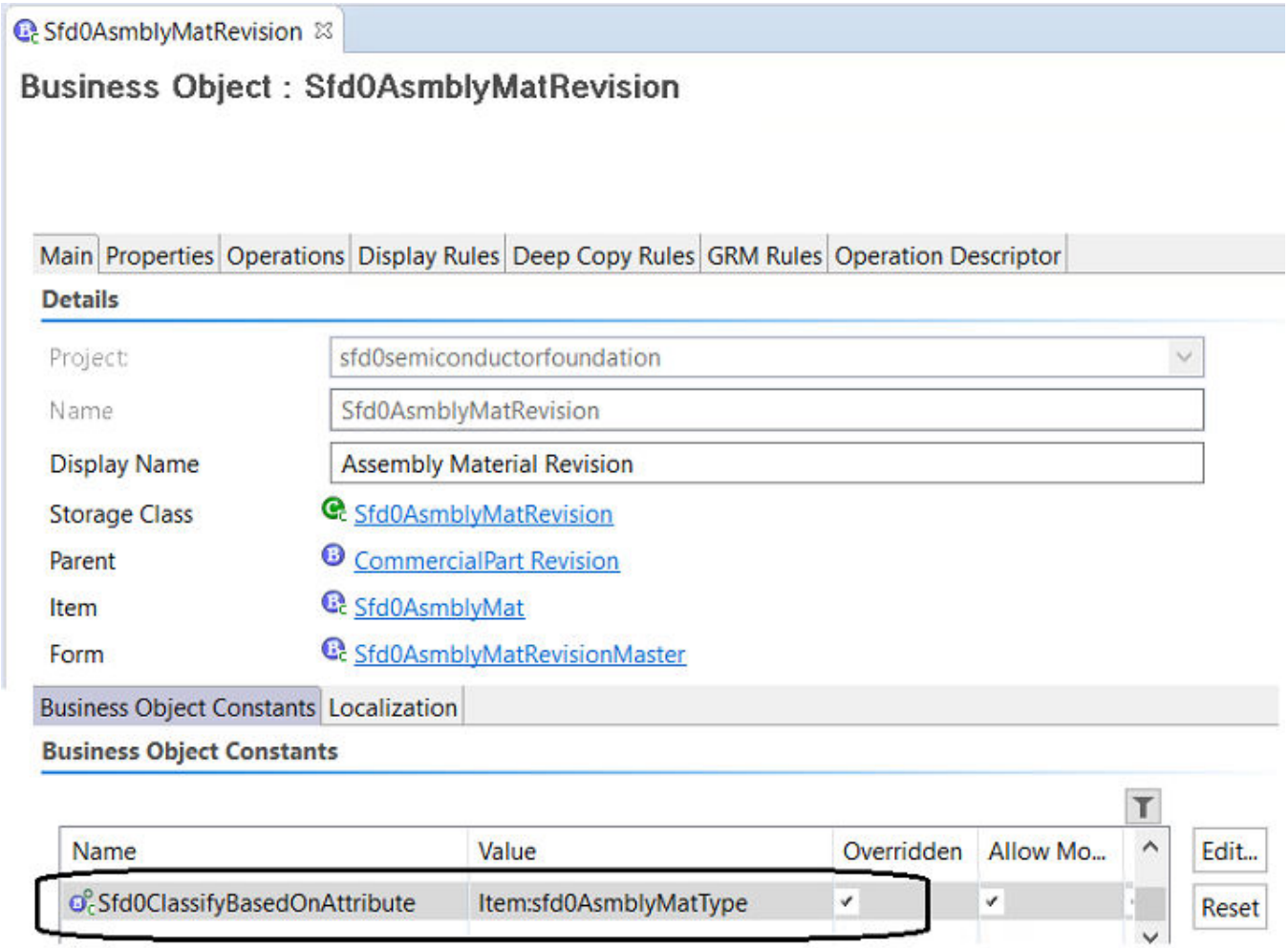
You must design and implement a classification schema according to your specific requirements. If these preferences are not populated, then these validations will not occur.

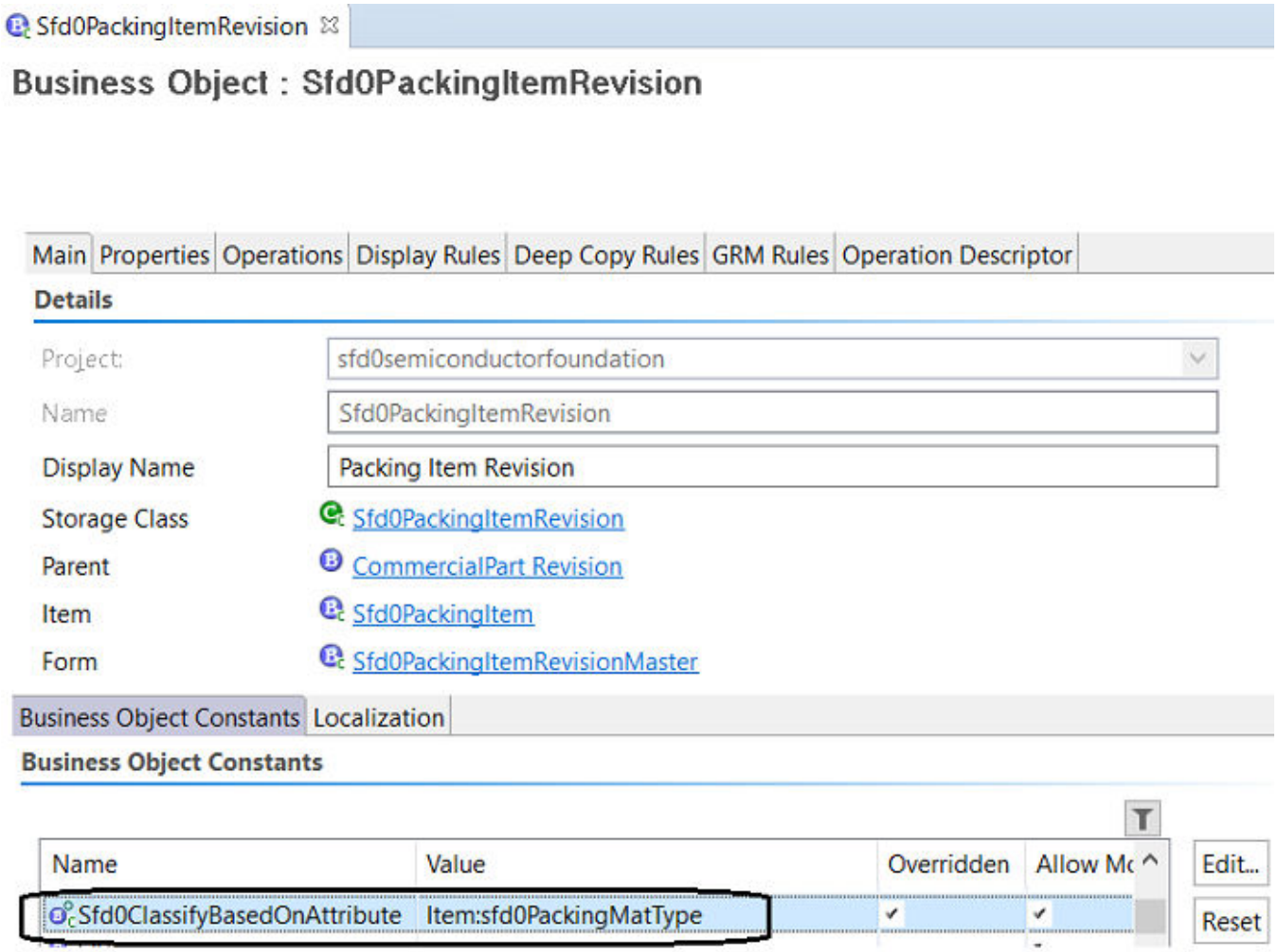
Classify on Create configuration

The configurations described in this topic enable auto-classification.

You can configure the **Sfd0ClassifyBasedOnAttribute** business object constant on the revision type of the BO of the property. Auto-classification is performed on this basis.

The value of the business constant attachment is **Item:** *<propertyName>* if the property is on the Item of the object that is the basis of the classification. The value of the business constant attachment will be **ItemRevision:** *<propertyName>* if the property is on the Item Revision of the object that is the basis of the classification. OOTB values are shown in the following figures.



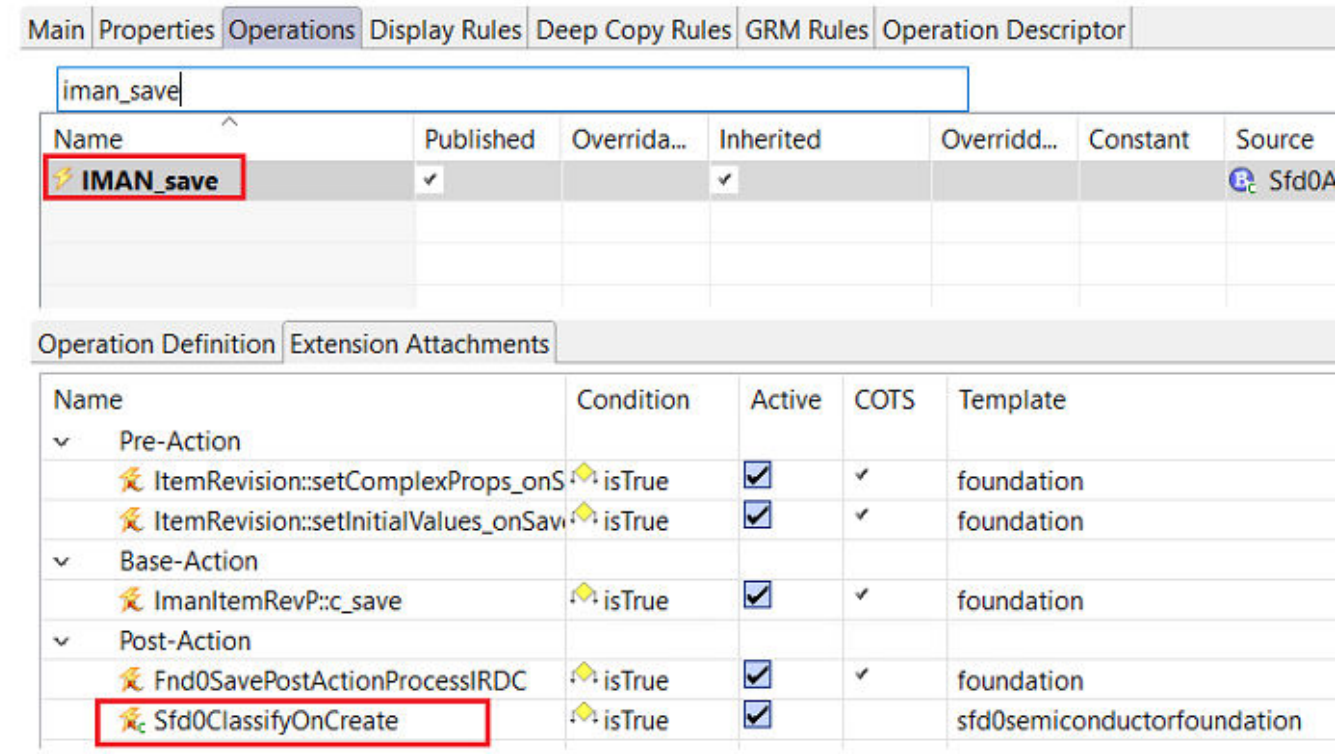


The **Sfd0_Auto_Classification_Class_Ids** preference should be configured with the mapping of attribute value and the classification class IDs used for auto-classification. The syntax of the preference value is **BoType:PropertyValue:Classification Class ID**.

> Example:
>
> **Sfd0AsmblyMatRevision:Bond Wire:ICM040101**

For auto-classification to be enabled on creation of a particular Item subtype, the extension **Sfd0ClassifyOnCreate** must be configured for the corresponding **ItemRevision** subtypes on the **IMAN_save** operation as a **PostAction** extension point.

The following example is the OOTB configuration for **Sfd0AsmblyRevision**.



Marking management

This section details the Marking Management configuration that is available to set up the Semiconductor Lifecycle Management solution according to your needs.

The Marking Template pattern can consist of combinations of the characters shown in the following table.

Character	Pattern match
&	Alphanumeric value
X	Uppercase alphabetic value or numeric value
x	Lowercase alphabetic value or numeric value
N	Numeric value
n	Numeric value
@	Alphabetic value
A	Uppercase alphabetic value
a	Lowercase alphabetic value

Character	Pattern match
U	Uppercase dynamic character
u	Lowercase dynamic character
D	Mixed case dynamic character
“string”	String delimiters. For example, if you want the word **Part** to appear in the naming rule, define it as **"Part"** in the naming rule pattern.
?	Any single character value
****	Escape the next character to have a literal meaning. This character is only required when using delimiters inside of other delimiters, for example, `"A\”Special\”Name"`, which matches `[A "Special" Name]`.

Marking Specification validation

You can control which type of Marking design revision can be attached to a Primary business object using the **Sfd0_Allowed_Marking_design_type** preference.

Panel Asset validation and content generation

The following configurable rules are provided on Marking SOA operations to meet the semiconductor industry process needs as defined in the solution guide.

- The operation validates the Marking specification value against the pattern defined in its respective marking template. You can turn the pattern matching check off or on using the **Sfd0_Panel_Matching_Pattern_Required** preference.

- You can change the schema for the generated XML file using the **Sfd0_marking_panel_content_schema** preference.